Air Force Institute of Technology

CSCE 525: Introduction to Cyber Warfare and Security

Nathan Flack

2 October 2018

CTC 2

**Question:** **Identify the top three cyber threats as they relate to a functional community of your choosing. Justify your prioritization of these threats based on associated risks and potential implications.**

I chose to examine cyber from the perspective of the nuclear community. Many nuclear control systems were developed before cyber threats were even on the radar. They were created to be stand-alone systems not connected to the Internet. Additionally, strong controls have been put in place to ensure a human is in the decision-making process when dealing with nuclear capabilities. I believe someone in the nuclear field would see cyber as strictly a means of communication connecting decision makers to operators enabling Command and Control or ways to connect sensors together to regulate nuclear plants. Many of the communication challenges revolve around communication in and through a nuclear event, which is a battle against the physical environment and not with actors in cyberspace. However, it seems as if a new era is emerging in nuclear cybersecurity.

First, nuclear systems are becoming more accessible to cyber actors as they become more connected. Patrick Tucker, a reporter for Defense One, identified calls from within the U.S. Government to create “more digital links between various parts of the nuclear enterprise.”[[1]](#footnote-1) While these new connections provide many important operational capabilities, the report makes clear that these actions could increase the attack vectors for our countries most expensive, powerful, and dangerous weapons.

Second, the worldwide nuclear community may be awakening to the potential issues that exist today and could be introduced in the future. In January 2018, Chatham House, an independent policy institute in London, England released a report titled “Cybersecurity of Nuclear Weapons Systems: Threats, Vulnerabilities, and Consequences,” which outlines the array of cyber risks, vulnerabilities, and considerations that nuclear states should consider while operating current nuclear capabilities and developing future systems. The report included a clear call to nuclear capable countries to reduce the cyber risk carried by their nuclear command, control, and communication systems. While many in the nuclear community might think that no other country or entity would dare to attack a nuclear capability because of the escalation it would cause, they should be very cautious. The report states, “It might seem likely that no country would be willing to face the consequences of starting a cyber offensive campaign in the nuclear weapons domain. However, an escalation is possible if cyber operations continue against key strategic assets of a country.”[[2]](#footnote-2) Outside control or influence on our cyber-enabled nuclear systems could spell disaster for the U.S. and other nuclear capable countries around the world.

1. Patrick Tucker, "As America's Nukes and Sensors Get More Connected, the Risk of Cyber Attack Is Growing," Defense One, January 17, 2018, 1, accessed October 03, 2018, https://www.defenseone.com/technology/2018/01/americas-nukes-and-sensors-get-more-connected-risk-cyber-attack-growing/145229/. [↑](#footnote-ref-1)
2. . Beyza Unal and Patricia Lewis, *Cybersecurity of Nuclear Weapons Systems: Threats, Vulnerabilities and Consequences,* International Security Department, Chatham House, January 2018, 15, accessed October 2, 2018, https://www.chathamhouse.org/sites/default/files/publications/research/2018-01-11-cybersecurity-nuclear-weapons-unal-lewis-final.pdf. [↑](#footnote-ref-2)